UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. GAMAL ABDELAZIZ, *et al*., Defendants	No. 1:19-CR-10080-NMG

GOVERNMENT'S NOTICE AND MOTION
REGARDING AUTHENTICATION

The government respectfully moves pursuant to Federal Rules of Evidence 902(11), 902(13), and 902(14), for an Order finding that the (a) phone calls and data intercepted pursuant to a wiretap of Rick Singer's telephone; (b) e-mail records obtained pursuant to search warrants; and (c) a forensic extraction of Singer's iPhone, including the extraction report and six voicemail messages extracted from the device, are authentic and that admission of the certificates of authenticity pertaining to this evidence does not violate the Confrontation Clause. The purpose of this motion is to save the Court's and jury's time and to avoid the need for testimony from multiple authentication witnesses at trial.[1] This motion also serves as notice to the defendants of the government's intent to authenticate the records under Federal Rules of Evidence 902(11), 902(13), and 902(14).[2]

[1] The witnesses will include agents from the New England Regional Computer Forensic Laboratory, the FBI's Telecommunications Intercept & Collection Technology Unit, as well as representatives of Google LLC and Microsoft Corp.

[2] The records to be authenticated by this motion have been produced to the defense.

Specifically, the United States moves to pre-authenticate the following records pursuant to Federal Rule of Evidence 902(11), 902(13), and 902(14):

(a) Data intercepted by wiretap: wire and electronic communications intercepted over the cellular telephone assigned the call number ending in 8802, used by William "Rick" Singer. *See* Exhibit A.

(b) E-mail records: e-mails (and associated attachments) obtained via searches of the following e-mail accounts: gamalaziz797@gmail.com; rickwsinger@gmail.com; rwsinger@gmail.com; and john@hyannisportcapital.com. *See* Exhibits B-D.

(c) iPhone image: a forensic extraction of Singer's iPhone, IMEI 353807081688088, including the extraction report and six voicemail messages extracted from the device. *See* Exhibit E.

The admissibility of the records at issue will still be subject to challenge by defense on the basis of hearsay and relevance. *See* Fed. R. Evid. 902(13), Advisory Committee's Note (2017) ("A certification under this Rule can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to admissibility of the proffered item on other grounds . . . .").

LEGAL STANDARD

Federal Rule of Evidence 902 addresses "evidence that is self-authenticating." Extrinsic evidence is not required for admission of evidence that is self-authenticating under Rule 902. "Certified domestic records of a regularly conducted activity" may be self-authenticated under Federal Rule of Evidence 902(11). The records must satisfy the business records requirements of Rule 803(6)(A)-(C), "as shown by a certification of custodian or qualified person." Fed. R. Evid. 902(11). Rule 803(6) provides that business records are admissible if they are accompanied by a certification of their custodian or other qualified person that satisfies three requirements: (A) that the records were "made at or near the time by – or from information transmitted by – someone

with knowledge"; (B) that they were "kept in the course of a regularly conducted activity of a business"; and (C) that "making the record was a regular practice of that activity."

Federal Rules of Evidence 902(13) and 902(14), which became effective in 2017, allow certain types of certified digital records and data to be self-authenticating, removing any need to provide extrinsic evidence of authenticity. Rule 902(13) provides that "certified records generated by an electronic process or system that produces an accurate result, shown by certification meeting requirements of Rule 902(11)" is self-authenticating. Rule 902(14) provides that "certified data copied from an electronic device, storage medium, or file" is self-authenticating if it is "authenticated by a process of digital identification, shown by certification meeting requirements of Rule 902(11)." The Rules Committee explained that "as with the provisions of business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary." Fed. R. Evid. 902(13), Ad. Comm. Note, 2017 Amendments. "It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented." *Id.* "The amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly." *Id.* *See also* Fed. R. Evid. 902(14), Ad. Comm. Note, 2017 Amendments (describing the rationale behind the new rule with substantially similar language).

ARGUMENT

A. The Court Should Find That The Records Are Self-Authenticating And No Witness Testimony Is Required For Their Authentication.

First, the government requests that the Court rule that the phone calls and data intercepted pursuant to a wiretap of Rick Singer's cellular telephone, assigned call number ending in 8802,

and certified pursuant to Rules 902(11) and 902(14) in Exhibit A, are *prima facie* authentic. The certification provided in Exhibit A establishes that (1) the surveillance in this case includes collections performed through the assistance of a wireless telecommunications service provider; (2) FBI receives the intercept from the provider over two separate channels, one for audio related to a phone call, and another for pen register and trap and trace data related to the call, as well as SMS (text message) communications; (3) the data are received within the FBI's telephone collection system, which is run by the Telecommunications Intercept & Collection Technology Unit; (4) the collected data is hashed and proprietary software is utilized to assign a unique digital signature to each call and text message; (5) the certifier reviewed the data associated with all of the sessions in this case; and (6) all of the digital signatures and hash values for the sessions the certifier has been asked to review have been verified as being intact.[3] A *prima facie* finding of authenticity would obviate the trial testimony of an FBI Supervisory Special Agent serving within the Telecommunications Intercept & Collection Technology Unit in the Operational Technology Division in Quantico, Virginia.

[3] *See* Fed. R. Evid. 902(14), Ad. Comm. Note, 2017 Amendment ("Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by 'hash value.' A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical. Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates. This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original. The rule is flexible enough to allow certifications through processes other than comparison of hash value.").

Second, the government requests that the Court rule that the e-mails obtained pursuant to search warrants executed on multiple e-mail accounts – gamalaziz797@gmail.com; rickwsinger@gmail.com; rwsinger@gmail.com; and john@hyannisportcapital.com – and certified pursuant to Rules 902(11) and 902(13) in Exhibits B through D, are *prima facie* authentic so that custodian witnesses from Google and Microsoft need not appear at trial.

Numerous courts, both in and outside the First Circuit, have found similar provider records authentic pursuant to Rule 803(6)(D) and Rule 902(11). *See, e.g.*, *United States v. Burgos-Montes*, 786 F.3d 92, 119 (1st Cir. 2015) (affirming use of phone provider records accompanied by a certification under Rule 902(11), even if the exhibits themselves were made to comply with a request from law enforcement) (citing *United States v. Cameron*, 699 F.3d 621, 641-42 (1st Cir. 2012)); *United States v. Gal*, 606 F. App'x 868, 875 (9th Cir. 2015) (affirming the admission of "emails based on Yahoo's affidavit" pursuant to Federal Rule of Evidence 902(11)); *United States v. Hassan*, 742 F.3d 104, 13 n.25 (4th Cir. 2014) (rejecting "appellants' contention that the Facebook and Google certification are insufficient because they were made for litigation purposes several years after the postings occurred" as "entirely unpersuasive").

Third, the government requests that the Court rule that the forensic extraction of Singer's iPhone, IMEI 353807081688088, the corresponding extraction report, and six voicemail messages extracted from the device, certified under Rules 902(11), 902(13), and 902(14) in Exhibit E, are *prima facie* authentic so that the agent who verified accuracy of the extraction need not appear at trial. The attached certification establishes that (1) a complete and accurate image of the iPhone was generated using an electronic process or system (specialized forensic software); and (2) the certifier is a qualified person who verified the accuracy of the result and that the six voicemail

messages were located on the device. Testimony at trial will establish that the FBI obtained the device from Singer.

B. The Court Should Find That The Government's Admission Of, And Reliance On, The Certificates Does Not Violate The Confrontation Clause.

As part of its Confrontation Clause jurisprudence, the Supreme Court has specifically distinguished affidavits or certificates authenticating records from other types of affidavits. *See Melendez-Diaz v. Massachusetts*, 557 U.S. 305 (2009). In *Melendez-Diaz*, the Court held that a particular affidavit prepared by a drug analyst as part of a criminal investigation was testimonial. *Id.* at 307. The affidavit stated that certain powder seized from a defendant was determined to be "cocaine." *Id.* In responding to the dissent's concern that the holding would eviscerate the usefulness of Rule 902(11), the Court explained that "[a] clerk could by affidavit authenticate or provide a copy of an otherwise admissible record, but could not do what the analysts did here: create a record for the sole purpose of providing evidence against a defendant. *Id.* at 322-23.

Relying on *Melendez-Diaz*, numerous Circuits and lower courts have concluded that certifications authenticating records are not testimonial and therefore are not barred by *Crawford v. Washington*, 541 U.S. 36 (2004). *See*, *e.g.*, *United States v. Johnson*, 688 F.3d 494, 504-05 (8th Cir. 2012); *United States v. Ellis*, 460 F.3d 920 (7th Cir. 2006). The *Ellis* Court explained that an authenticating certification under Rule 902(11) is "nothing more than the custodian of records . . . attesting that the submitted documents are actually records kept in the ordinary course of business" and "merely establish the existence of the procedures necessary to create a business record." 460 F.3d at 927. It is the underlying records, not the certification, that are introduced to establish the facts at trial. *See also United States v. Brinson*, 2014 WL 6872171 (10th Cir. Dec. 8, 2014 (holding that *Melendez-Diaz* did not apply because the certificate authenticating debit card records did not contain any analysis that would constitute out-of-court testimony but was simply a non-testimonial

statement of authenticity) (citing *United States v. Yeley-Davis*, 632 F.3d 673, 680-81 (10th Cir. 2011)).

The Court should hold that the admission of the certificates discussed above to authenticate the calls and data intercepted pursuant to wiretap, e-mails seized pursuant to search warrants, and the extraction of Singer's iPhone does not violate the Confrontation Clause.

CONCLUSION

For the foregoing reasons, the government respectfully requests that the Court make a *prima facie* finding that the (a) intercepted wire and electronic communications over the cellular telephone assigned the call number ending in 8802, used by Rick Singer; (b) e-mails obtained via searches of the e-mail accounts gamalaziz797@gmail.com; rickwsinger@gmail.com; rwsinger@gmail.com; and john@hyannisportcapital.com, and (c) a forensic extraction of Singer's iPhone, IMEI 353807081688088, including the extraction report and six voicemail messages extracted from the device, are authentic, that admission of certificates to authenticate the underlying records does not violate the Confrontation Clause, and that live witness testimony to authenticate these records is unnecessary.

Respectfully submitted,

NATHANIEL R. MENDELL
Acting United States Attorney

By: */s Stephen E. Frank*
JUSTIN D. O'CONNELL
LESLIE A. WRIGHT
KRISTEN A. KEARNEY
IAN J. STEARNS
STEPHEN E. FRANK
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/Stephen E. Frank
STEPHEN E. FRANK